#4

SPECIFICATION
[Electronic Version 1.2.8]

A PORTABLE KEYING DEVICE AND METHOD

[h1] Background of the Invention

[p1] The present invention relates generally to transaction terminals, and particularly to the installation of security keys in transaction terminals.

[p2] Electronic terminals such as point-of-sale (POS) terminals are becoming ubiquitous in our society. These terminals include credit, debit, and check authorization capabilities. Some of these devices are used as stand-alone devices and some are networked using LAN technology. Because of the sensitive financial information being transmitted and received by these electronic terminals, security is a critical issue. In order to provide security, electronic terminals employ data encryption. Encryption devices scramble readable data to produce cipher text. Most of the terminals use an encryption key as part of the encryption process. An encryption key is a block of data that is combined with the readable input data to produce the cipher text. For example, the encryption key and the input data can be combined using an exclusive-OR function. On the other hand, the Data Encryption Standard (DES) algorithm is often used to combine an encryption key with input data to produce the cipher text. The DES algorithm employs a 56-bit encryption key to produce the cipher text. The use of an encryption key is considered to be more secure than scrambling the input data

[p3] Another security issue relates to tamper protection. Typically, all secure information such as encryption keys are stored in SRAM or PROM. In one approach, if the processor detects a downloading operation that may result in security information being compromised, the processor deletes the security information.

[p4] In another approach, tamper detection switches are employed to prevent physical tampering of the terminal. If the top enclosure of the terminal is separated from the main printed circuit board, or if the "trap door" is opened in the bottom of the enclosure, the detection switches are thrown. The operating system of the terminal is programmed to erase the security information in response to the signals received from the switches. In another approach, ultrasonic bonding is often used to provide evidence that someone attempted to open the terminal device.

[p5] While the above described methods are effective in terms of preventing or monitoring tampering, there are problems associated with these methods. Under certain

circumstances the security information loaded into the electronic terminal must be changed or updated. Oftentimes it is desirable to change the security information loaded into the electronic terminal at the factory before the first use. At this point, the terminal must be shipped to the factory or to a servicing organization to be re-programmed. Subsequently, the terminal is unboxed, the anti-tampering features are de-activated, the security information is reloaded, the terminal re-bonded and the terminal is repackaged. These steps are inefficient, time consuming and costly.

[p6] What is needed is a method of securely reprogramming the security information in an electronic terminal without having to remove the terminal from its shipping container, dismantle the terminal, de-activate the anti-tampering features, reload the security information, and re-bond the terminal. Further, what is needed is a method of securely reprogramming the security information in an electronic terminal without having to ship the terminal off-site.

[h2] Brief Summary of the Invention

[p7] The present invention addresses the needs discussed above. The present invention provides a system and method for securely reprogramming the security information in an electronic terminal without having to ship the terminal off-site. The present invention provides a system and method for securely reprogramming the security information in an electronic terminal without having to remove the terminal from its shipping container, dismantle the terminal, de-activate the anti-tampering features, reload the security information, and re-bond the terminal.

[p8] In another aspect, the present invention includes a method for installing a data communications encryption key in an electronic terminal. The electronic terminal including a secure encryption key memory location for storing the at least one data communications encryption key. The method includes: providing a portable keying device, whereby the portable keying device is physically separated from the electronic terminal; performing a handshaking routine, whereby the keying device and the electronic terminal exchange handshaking messages; transmitting an encryption key from the portable keying device to the electronic terminal; and storing the encryption key transmitted from the portable keying device to the electronic terminal in the secure key memory location.

[p9] In yet another aspect, the present invention includes a portable key installation system for installing a data communications encryption key. The system includes at least one electronic terminal having a secure encryption key memory adapted to store the at least one data communications encryption key, and a terminal communications unit coupled to the secure encryption key memory. A portable keying device includes a memory adapted to store the at least one data communications encryption key, and a device communications unit coupled to the memory device, the device communications unit being adapted to bi-directionally communicate the at least one

data communications encryption key in a predetermined format to the terminal communications unit.

[p10] Additional features and advantages of the invention will be set forth in the detailed description which follows, and in part will be readily apparent to those skilled in the art from that description or recognized by practicing the invention as described herein, including the detailed description which follows, the claims, as well as the appended drawings.

[p11] It is to be understood that both the foregoing general description and the following detailed description are merely exemplary of the invention, and are intended to provide an overview or framework for understanding the nature and character of the invention as it is claimed. The accompanying drawings are included to provide a further understanding of the invention, and are incorporated in and constitute a part of this specification. The drawings illustrate various embodiments of the invention, and together with the description serve to explain the principles and operation of the invention.

[h3] Brief Description of the Drawings

[p12] Figure 1 is a diagrammatic depiction of a portable key installation system in accordance with one embodiment of the present invention;

[p13] Figure 2 is a perspective view of a portable key installation system depicted in Figure 1;

[p14] Figure 3 is a chart showing a method for installing a security key in an electronic terminal using a portable device;

[p15] Figures 4A and 4B are a diagrammatic depictions of an electronic terminal in accordance with a second embodiment of the present invention;

[p16] Figure 5 is a diagrammatic depiction of an electronic terminal in accordance with a third embodiment of the present invention; and

[p17] Figure 6 is a diagrammatic depiction of an electronic terminal in accordance with a fourth embodiment of the present invention.

[h4] Detailed Description of the Invention

[p18] Reference will now be made in detail to the present exemplary embodiments of the invention, examples of which are illustrated in the accompanying drawings.

Wherever possible, the same reference numbers will be used throughout the drawings to refer to the same or like parts. An exemplary embodiment of the portable key installation system of the present invention is shown in Figure 1, and is designated generally throughout by reference numeral 10.

[p19] In accordance with the invention, the present invention for a portable key installation system includes a portable keying device for installing a data communications encryption key in an electronic terminal. The electronic terminal including a secure encryption key memory location for storing the at least one data communications encryption key. The portable keying device includes a memory for storing the at least one data communications encryption key. A processor that is operative to generate a secure installation message, the secure installation message including the at least one data communications encryption key. A communications unit is coupled to the processor. The communications unit is operative to transmit the installation message in a predetermined format to the electronic terminal.

[p20] Thus, the present invention provides a system and method for securely reprogramming the security information in an electronic terminal without having to ship the electronic terminal off-site. The present invention provides a system and method for securely reprogramming the security information in an electronic terminal without having to remove the electronic terminal from its shipping container, dismantle the terminal, de-activate the anti-tampering features, reload the security information, and re-bond the terminal.

[p21] As embodied herein, and depicted in Figure 1 a diagrammatic depiction of a portable key installation system in accordance with one embodiment of the present invention is disclosed. System 10 includes portable keying device 100 and electronic terminal 200.

[p22] Portable keying device 100 includes I/O circuit 12, processor 14, RAM 16, EROM 18, key memory 20 and RF controller 22 coupled by way of system bus 28. RF controller 22 is connected to RF transceiver 24. RF transceiver 24 is connected to antenna 26. In one embodiment, I/O circuit 12 is coupled to a keypad which is used to input the encryption key. In another embodiment, I/O circuit 12 is coupled to a connector that mates with an external device. The encryption key is downloaded from the external device into key memory 20 via I/O circuit 12. In yet another embodiment, an initial key download is performed via the keypad or the external device. Subsequently, processor 14 uses the initial key to generate encryption keys for a plurality of devices by running a secure key generation algorithm.

[p23] It will be apparent to those of ordinary skill in the pertinent art that modifications and variations can be made to processor 14 of the present invention depending on cost and programming considerations. For example, in one embodiment processor 14 is implemented using an 8-bit "programmable system-on-a-chip" device, of the type manufactured by Cypress Semiconductor. One of ordinary skill in the art will recognize that 16-bit and 32-bit devices can also be used, in addition to other 8-bit

devices.

[p24] It will be apparent to those of ordinary skill in the pertinent art that modifications and variations can be made to EROM 18 and key memory 20 of the present invention depending on cost, security, and re-programmability considerations. In one embodiment key memory 20 is actually a memory location within EROM 18. For example, in the 8-bit micro-controller embodiment, EROM 18 and key memory 20 are implemented using 32kbytes of embedded ROM. Ram 16 is implemented using 1kbyte of embedded RAM. In another embodiment, key memory 20 is implemented using a separate memory device. In general key memory 20 is implemented using non-volatile memory such as E2PROM, Flash EPROM, battery-backed RAM, or Ferro RAM (FRAM). Re-programmability is an issue in the keying device because the device is re-usable to reprogram any number of terminals 200.

[p25] It will be apparent to those of ordinary skill in the pertinent art that modifications and variations can be made to RF controller 216, RF transceiver 218, and antenna 220 of the present invention depending on cost and implementation considerations. For example, in Figure 1 and Figure 2, a low power/close proximity RF system is depicted. In this embodiment, transceiver 24 outputs approximately 1 milli-Watt and has an effective range of about 1 meter of less. In another embodiment, the RF components are replaced altogether by an infrared optical communications system. In yet another embodiment, the RF components are replaced by an audio communications system that employs DTMF technology.

[p26] Referring back to Figure 1, any type of electronic terminal 200 can be employed in system 10 of the present invention. In one embodiment, electronic terminal 200 is a simple hard-wired terminal. In other embodiments, terminal 200 is a keypad, signature pad, card reader, bar code reader, or a POS retail transaction terminal. In yet another embodiment, electronic terminal 200 is a stand-alone unit. In an alternate embodiment, electronic terminal 200 is networked to a LAN. In the example depicted in Figure 1, electronic terminal 200 includes I/O circuit 202, processor 204, RAM 206, EROM 208, key memory 214 and RF controller 216 coupled by way of system bus 222. In this example, terminal 200 includes imaging assembly 208 for image scanning purposes. Image assembly 208 is controlled by processor 204. Imaging data generated by image assembly 208 is written into RAM 206 by way of DMA channel 210. RF controller 216 is connected to RF transceiver 218. RF transceiver 218 is connected to antenna 220.

[p27] In another embodiment, processor 204 includes a general purpose processor and an additional processor to handle secure information including the encryption key. In this embodiment, the additional processor is programmed to handle I/O functions involving a keypad and display. Key memory 214 is embedded in the security processor.

[p28] It will be apparent to those of ordinary skill in the pertinent art that modifications and variations can be made to key memory 214 of the present invention depending on

cost, security, and re-programmability considerations. In one embodiment key memory 214 is actually a memory location within EROM 18. In another embodiment, key memory 214 is implemented using a separate memory device. In general key memory 214 is implemented using non-volatile memory such as E2PROM, Flash EPROM, battery-backed SRAM, or Ferro RAM (FRAM). One of the re-programmability considerations relates to the programming voltage required by key memory 214. Some memory devices require an additional programming voltage, over and above the normal system operating voltage, before being enabled to reprogram the contents of the memory.

[p29] With respect to the other components of terminal 200 depicted in Figure 1, modifications and variations are dependent on the type and complexity of terminal 200. Further, the communications components are dependent on the type of communications components present in portable keying device 100.

[p30] As embodied herein, and depicted in Figure 2, a perspective view of the portable key installation system depicted in Figure 1 is disclosed. Electronic terminal 200 includes housing 230, which accommodates keypad 232, display 234, card reader 236, cable 238 and antenna 220. As discussed above, terminal 200 can be a stand-alone terminal or a networked device. Portable keying device 100 includes housing 102, keypad 120 and liquid crystal display 122. Figure 2 illustrates a secure communications protocol that avoids accidental erasure or reprogramming of the encryption key stored in key memory 214. In this embodiment, additional security is provided by keying system 10 by employing RF components that include proximity features. The proximity features include power level S, angular directivity 2, and polarity P. Of course, the effective range of keying device 10 is a function of the power. If, for example, portable keying device 100 is not within 1 meter, and is not pointing at antenna 220 (within, e.g., "15o), and does not emit an RF signal having a polarity that is matched to the RF system in terminal 200, the re-programming attempt will be unsuccessful.

[p31] As embodied herein, and depicted in Figure 3, a chart showing a method for installing a security key in an electronic terminal using a portable device is disclosed. In step S300, portable device 100 and electronic terminal exchange handshaking messages. First, portable device 100 must satisfy the distance, angular directivity, and polarity requirements discussed above. Second, portable device 100 and electronic terminal 200 exchange authentication codes. Subsequently, in step S302, portable device 100 transmits an authorization code to electronic terminal 200. The transmitted authorization code must match the authorization code stored in EROM 212 of terminal 200. If the authorization codes match, portable device 100 transmits an installation message in step S304. The installation message includes the encryption key to be installed. In step S306, terminal 200 retransmits the encryption key to portable device 100. Portable device 100 validates the key by comparing the key that it received from terminal 200 in step S306 with the key it sent to terminal 200 in step S304. If the two keys do not match, portable device 100 performs step S304 over again. As shown in steps S308 - S314, device 100 displays an error message to the user after several unsuccessful attempts, indicating that a successful transfer of the

key could not be performed. If the key is validated in step S306, processor 204 writes the encryption key into secure key memory 214 in step S316.

[p32] In an alternate embodiment, step S306 includes additional steps. Portable device 100 transmits a test encryption key that it believes is currently being stored in key memory 214. If the test encryption key matches the current encryption key, terminal 200 transmits an acknowledgement signal. If the keys do not match, the installation procedure is aborted. Upon receiving the acknowledgement signal, portable device 100 transmits the new encryption key to terminal 200. If the new key is validated in step S306, processor 204 writes the encryption key into secure key memory 214, and the procedure is complete.

[p33] As embodied herein, and depicted in Figure 4A, a diagrammatic depiction of electronic terminal 200 in accordance with a second embodiment of the present invention is disclosed. In this embodiment, key memory 214 requires an external programming voltage. As described above, terminal 200 includes processor 204, key memory 214, transceiver 218 and antenna 220. In this example it is assumed that terminal 200 is boxed in a shipping container of some sort. Thus, terminal 200 is not connected to any external power supply. However, terminal 200 includes diode 240, normal operating voltage supply 250 and programming voltage supply 260. Normal operating voltage supply 250 includes capacitor 252, capacitor 254, and voltage regulator 256. Programming operating voltage supply 260 includes capacitor 262, capacitor 264, and voltage regulator 266. When portable device 100 transmits an RF signal to terminal 200, diode 240 rectifies the AC-RF signal and prevent any return signal from damaging the RF components. The resultant DC signal is used to charge up capacitors 252, 254, 262 and 264. Voltage regulator 256 ensures that the power supplied to terminal 200 is within system operating parameters. Voltage regulator 266 ensures that memory 214 receives an acceptable programming voltage. In response to the normal operating voltage supplied by supply 250, terminal 200 is energized and ready for key installation. At the proper time, e.g. during step S308 (See Figure 3), processor 204 activates switch 262 and supply 260 provides memory 214 with the programming voltage required to store the new encryption key therein. Figure 4B is an alternative embodiment of Figure 4A. In the alternative embodiment, switch 262 is connected to the output of normal operating voltage supply 250 instead of being connected to the input of key memory 214 as in Figure 4A. Functionally, there is very little difference between the two alternative embodiments.

[p34] As embodied herein, and depicted in Figure 5, a diagrammatic depiction of an electronic terminal in accordance with a third embodiment of the present invention is disclosed. In this embodiment, battery 242 is included within terminal 200 to provide a normal operating voltage. Diode 240 is included to rectify the RF signal and prevent any return signals from damaging the RF components. Programming operating voltage supply 250 is included to provide programming voltage to key memory 214. Programming operating voltage supply 250 includes capacitor 254, capacitor 256, and voltage regulator 258. When portable device 100 transmits an RF signal to terminal 200, diode 240 rectifies the AC-RF signal. The resultant DC signal

is used to charge up capacitors 254 and 256. Again, at the proper time, e.g. during step S308 (See Figure 3), processor 204 activates switch 252 and supply 250 provides memory 214 with the programming voltage required to store the new encryption key therein.

[p35] As embodied herein, and depicted in Figure 6, a diagrammatic depiction of an electronic terminal in accordance with a fourth embodiment of the present invention is disclosed. In this embodiment, the required programming voltage is supplied internally. Battery 240 is included within terminal 200 to provide both the normal operating voltage and the programming voltage. In this embodiment battery 240 is coupled to programming voltage supply 250. Programming voltage supply 250 is identical to those depicted in Figure 4 and Figure 5. Since battery 240 supplies DC voltage to capacitors 254 and 256, no rectifying diode is needed. Yet again, at the proper time, e.g. during step S308 (See Figure 3), processor 204 activates switch 252 and programming supply 250 provides memory 214 with the programming voltage required to store the new encryption key therein.

[p36] It will be apparent to those skilled in the art that various modifications and variations can be made to the present invention without departing from the spirit and scope of the invention. Thus, it is intended that the present invention cover the modifications and variations of this invention provided they come within the scope of the appended claims and their equivalents.